PDR RID Report

Originator	Smith, Gerald	**Phone No**	301-982-5414
Organization	Intermetrics, Inc.		
E Mail Address	6301 Ivy Lane, Suite 200, Greenbelt, MD 20770		
Document	EOC LAN Design		

RID ID **PDR** 48
Review FOS
Originator Ref IVV-GSS-02
Priority 2

Section NA **Page** DJM-3 **Figure Table** NA

Category Name	Design	**Actionee**	HAIS
Sub Category			
Subject	Security Aspects of IST Connectivity to EOC LAN		

Description of Problem or Suggestion:

The presentation showed that one possible connection for ISTs to the EOC LAN would be through routers which direct users to the Operational LAN. Are there any security tradeoffs by having ISTs connect through the Support LAN rather than directly to the Operational LAN? It would seem that routing ISTs through the Support LAN, if performance was not an issue, might add an additional barrier. Would it not be preferable for an intruder to end up in the Support LAN if he/she was able to breach security. It would seem prudent to keep the Operational LAN as "clean" as possible of external gateways to ensure its integrity.

Originator's Recommendation

Review the security aspects of having ISTs access the EOC through routers either in the Operational or Support LANs.

GSFC Response by: **GSFC Response Date**

HAIS Response by: D. Herring **HAIS Schedule** 1/20/95

HAIS R. E. A. Miller **HAIS Response Date** 1/23/95

The ISTs must have access to the Operational LAN in order to receive real-time telemetry, which is available only via the Operational Net. The ISTs may (this is being worked for FOS CDR) have direct access to the Support LAN as well. This would be accomplished by attaching the Support LAN FDDI to a second interface on the EOC Router.

Several security measures are involved in assuring EOC integrity. The first occurs at the network layer and involves filtering at the EOC Router. Filters in the router will allow only pre-defined IST hosts access to the EOC; all other hosts will not be allowed in.

The second measure involves authenticating the IST User. This is done via DCE-based Kerberos encryption which does not allow the user's password to ever appear on the network. The third measure authorizes the user to perform only those actions he is allowed to perform. This is realized through the use of DCE Access Control Lists (ACLs).

The final security measure involves insuring that data is not modified during its transit across the network to the EOC. This can be accomplished by the use of encrypted checksums within inter-process communications. There are several COTS software products available that perform checksum encryption (e.g., DCE, Hughes Netlock, Northern Telecom Entrust).

FOS feels that these measures provide a solid security foundation that will prevent unauthorized access or use of the EOC.

Status **Closed** **Date Closed** **2/1/95** **Sponsor** **Johns**

****** **Attachment if any** ******